Distributed Systems

Introduction to Cryptography

Paul Krzyzanowski
pxk@cs.rutgers.edu

Ngywioggazhon Pystemp

Auesfnsicutiwf & Moiiunocaiwn
Piqtoaoyp

Cryptographic Systems

Authentication & Communication
Protocols

---

cryptography
↙ ↘
κρυπτός γραφία
↓ ↓
hidden writing

A secret manner of writing, … Generally, the art of writing or solving ciphers.
— Oxford English Dictionary

---

cryptology
↙ ↘
κρυπτός λογια
↓ ↓
hidden speaking

1967 D. Kahn, *Codebreakers* p. xvi, Cryptology is the science that embraces cryptography and cryptanalysis, but the term ‘cryptology’ sometimes loosely designates the entire dual field of both rendering signals secure and extracting information from them.
— Oxford English Dictionary

Cryptography ≠ Security

Cryptography may be a component of a secure system

Adding cryptography may not make a system secure

Terms

Plaintext (cleartext), message M

encryption, E(M)

produces ciphertext, C=E(M)

decryption: M=D(C)

Cryptographic algorithm, cipher

Terms: types of ciphers

- restricted cipher
- symmetric algorithm
- public key algorithm

Restricted cipher

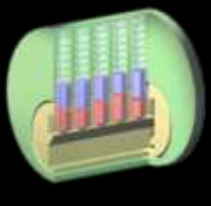
Secret algorithm

- Leaking
- Reverse engineering
  - HD DVD (Dec 2006) and Blu-Ray (Jan 2007)
  - RC4
  - All digital cellular encryption algorithms
  - DVD and DIVX video compression
  - Firewire
  - Enigma cipher machine
  - Every NATO and Warsaw Pact algorithm during Cold War

The key

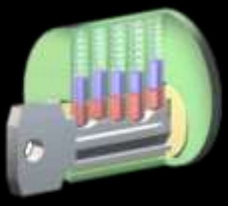
BTW, the above is a *bump key*. See http://en.wikipedia.org/wiki/Lock_bumping.

The key



Source: en.wikipedia.org/wiki/Pin_tumbler_lock

The key



Source: en.wikipedia.org/wiki/Pin_tumbler_lock

The key

- We understand how it works:
  - Strengths
  - Weaknesses
- Based on this understanding, we can assess how much to trust the key & lock.

Source: en.wikipedia.org/wiki/Pin_tumbler_lock

Symmetric algorithm

Secret key

$$C = E_K(M)$$

$$M = D_K(C)$$

Public key algorithm

Public and private keys

$$C_1 = E_{public}(M)$$
$$M = D_{private}(C_1)$$

also:

$$C_2 = E_{private}(M)$$
$$M = D_{public}(C_2)$$

McCarthy's puzzle (1958)

The setting:

- Two countries are at war
- One country sends spies to the other country
- To return safely, spies must give the border guards a password

- Spies can be trusted
- Guards chat – information given to them may leak

McCarthy's puzzle

Challenge

How can a guard authenticate a person without knowing the password?

Enemies cannot use the guard's knowledge to introduce their own spies

Solution to McCarthy's puzzle

Michael Rabin, 1958

Use one-way function, $B = f(A)$
- Guards get B …
  - Enemy cannot compute A
- Spies give A, guards compute $f(A)$
  - If the result is B, the password is correct.

Example function:

Middle squares
- Take a 100-digit number (A), and square it
- Let B = middle 100 digits of 200-digit result

One-way functions

- Easy to compute in one direction
- Difficult to compute in the other

Examples:

Factoring:

$pq = N$ EASY

find p,q given N DIFFICULT

Discrete Log:

$a^b \bmod c = N$ EASY

find b given a, c, N DIFFICULT

McCarthy's puzzle example

Example with an 18 digit number

A = 289407349786637777

A^2 = 83756614110525308948445338203501729

Middle square, B = 110525308948445338

Given A, it is easy to compute B

Given B, it is extremely hard to compute A

More terms

- one-way function
  - Rabin, 1958: McCarthy's problem
  - middle squares, exponentiation, …
- **[one-way] hash function**
  - message digest, fingerprint, cryptographic checksum, integrity check
- encrypted hash
  - message authentication code
  - only possessor of key can validate message

More terms

- Stream cipher
  - Encrypt a message a character at a time
- Block cipher
  - Encrypt a message a chunk at a time

Yet another term

- Digital Signature
  - Authenticate, not encrypt message
  - Use pair of keys (private, public)
  - Owner encrypts message with private key
  - Sender validates by decrypting with public key
  - Generally use *hash*(message).

Cryptography: what is it good for?

- Authentication
  - determine origin of message
- Integrity
  - verify that message has not been modified
- Nonrepudiation
  - sender should not be able to falsely deny that a message was sent
- Confidentiality
  - others cannot read contents of the message

Cryptographic toolbox

- Symmetric encryption
- Public key encryption
- One-way hash functions
- Random number generators

Classic Cryptosystems

Substitution Ciphers

Cæsar cipher

Earliest documented military use of cryptography
  - Julius Caesar c. 60 BC
  - shift cipher: simple variant of a substitution cipher
  - each letter replaced by one *n* positions away modulo alphabet size
    - *n* = shift value = key

Similar scheme used in India
  - early Indians also used substitutions based on phonetics
    - similar to pig latin

Last seen as ROT13 on Usenet to keep the reader from seeing offensive messages unwillingly

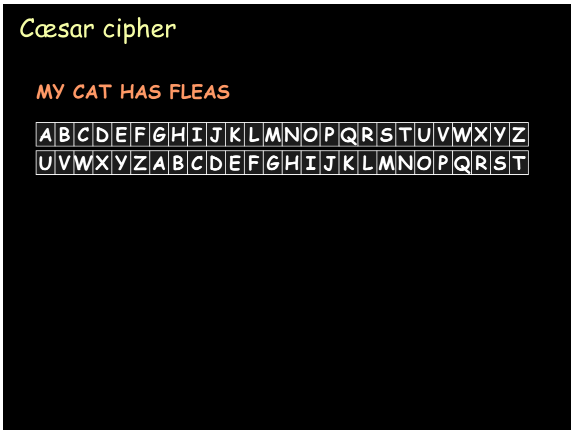
Cæsar cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Cæsar cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

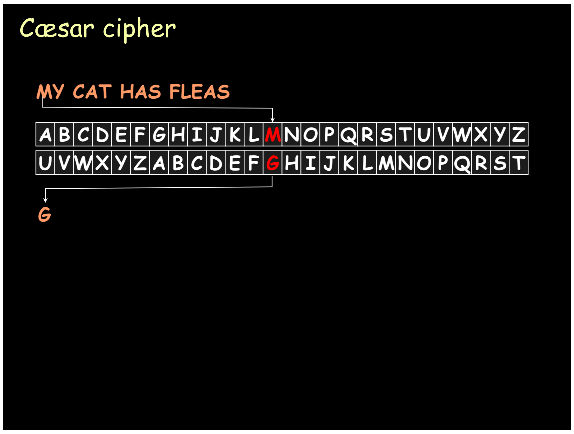
→ *shift alphabet by n (6)*



Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

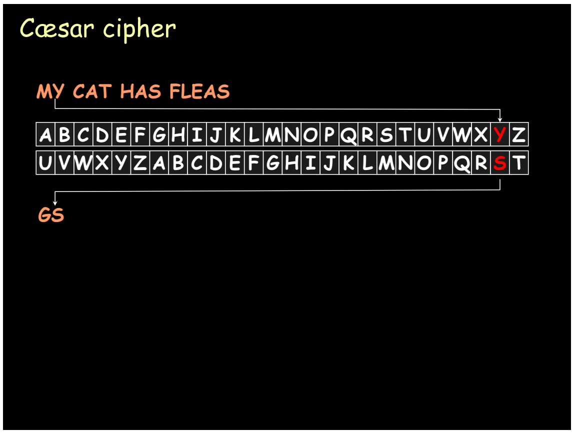


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

G

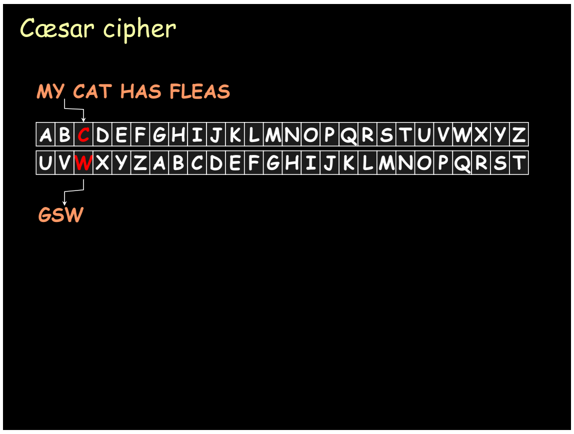


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GS

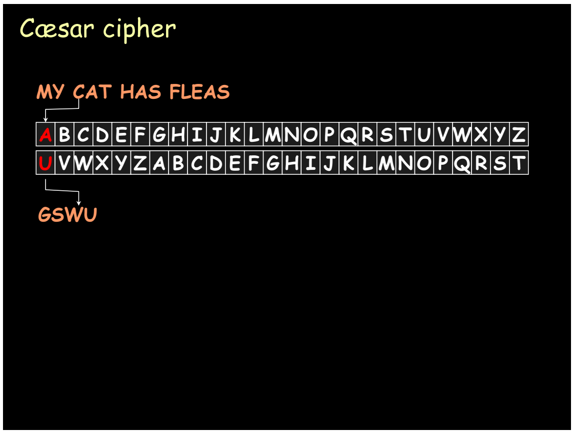


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSW

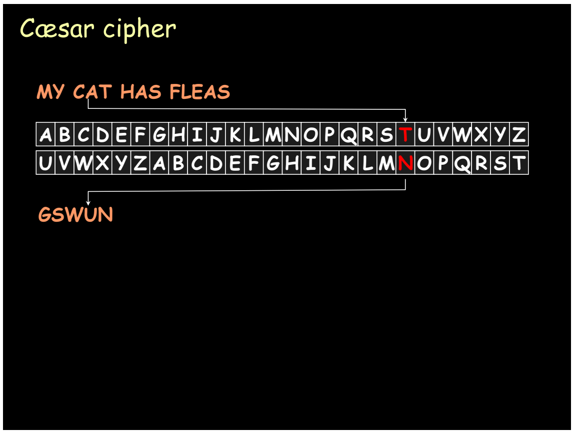


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWU

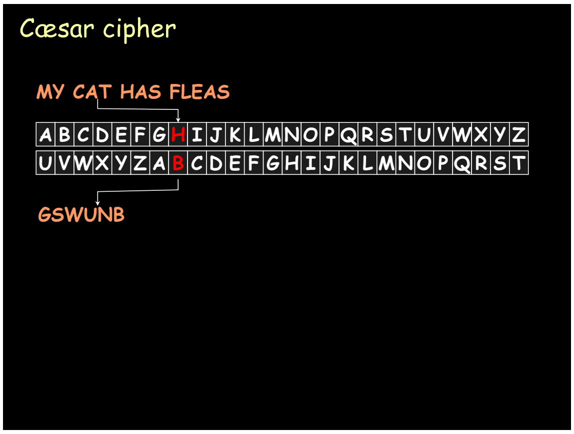


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUN

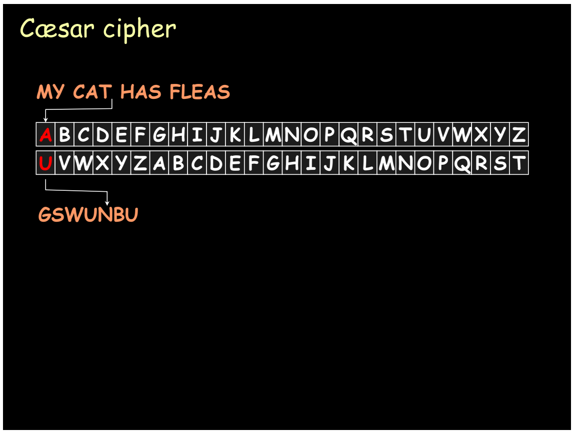


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUNB

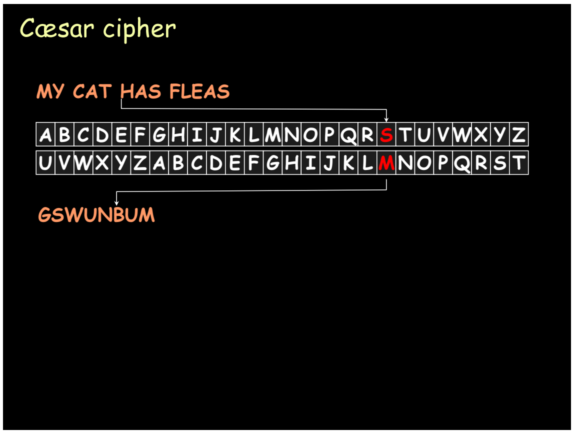


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUNBU

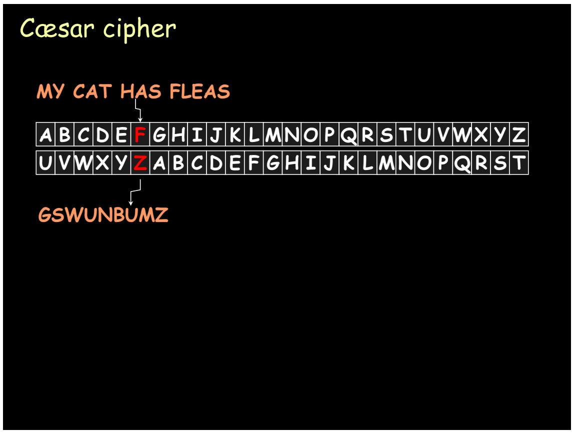


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUNBUM

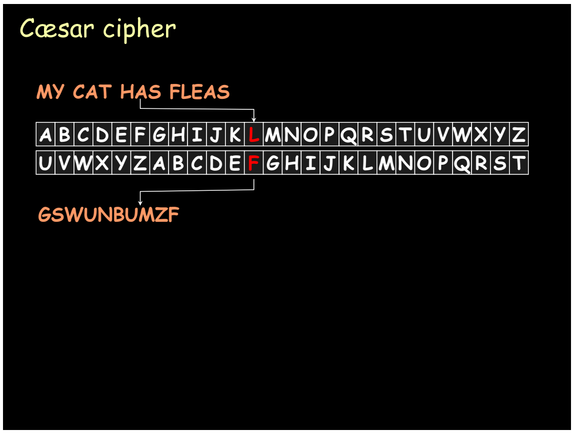


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUNBUMZ

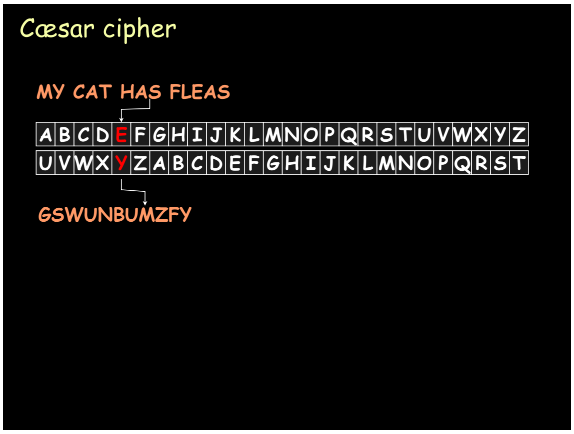


Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUNBUMZF



Cæsar cipher

MY CAT HAS FLEAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUNBUMZFY

Cæsar cipher

MY CAT HAS FLEAS

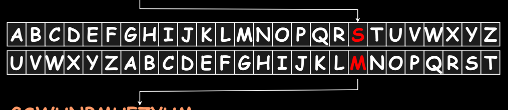
ABCDEFGHIJKLMNOPQRSTUVWXYZ

UVWXYZABCDEFGHIJKLMNOPQRST

GSWUNBUMZFYU

Cæsar cipher

MY CAT HAS FLEAS



ABCDEFGHIJKLMNOPQRSTUVWXYZ

UVWXYZABCDEFGHIJKLMNOPQRST

GSWUNBMUFZYUM

Cæsar cipher

MY CAT HAS FLEAS

ABCDEFGHIJKLMNOPQRSTUVWXYZ

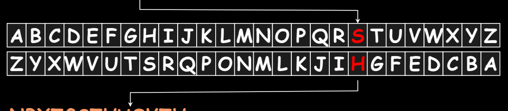
UVWXYZABCDEFGHIJKLMNOPQRST

GSWUNBMUFZYUM

- Convey one piece of information for decryption: *shift value*
- trivially easy to crack (26 possibilities for a 26 character alphabet)

Ancient Hebrew variant (ATBASH)

MY CAT HAS FLEAS



ABCDEFGHIJKLMNOPQRSTUVWXYZ

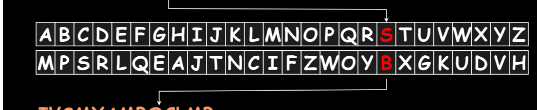
ZYXWVUTSRQPONMLKJIHGFEDCBA

NBXZGSZHUOVZH

- c. 600 BC
- No information (key) needs to be conveyed!

Substitution cipher

MY CAT HAS FLEAS



ABCDEFGHIJKLMNOPQRSTUVWXYZ

MPSRLQEAJTNCIFZWOYBXGKUDVH

IVSMXAMBQCLMB

- General case: arbitrary mapping
- both sides must have substitution alphabet

Substitution cipher

Easy to decode:

- vulnerable to frequency analysis

Moby Dick (1.2M chars)		Shakespeare (55.8M chars)	
e	12.300%	e	11.797%
o	7.282%	o	8.299%
d	4.015%	d	3.943%
b	1.773%	b	1.634%
x	0.108%	x	0.140%

Statistical Analysis

Letter frequencies

E: 12%

A, H, I, N, O, R, S, T: 6 – 9%

D, L: 4%

B, C, F, G, M, P, U, W, Y: 1.5 – 2.8%

J, K, Q, V, X, Z: < 1%

Common digrams:

TH, HE, IN, ER, AN, RE, …

Common trigrams

THE, ING, AND, HER, ERE, …

Polyalphabetic ciphers

Designed to thwart frequency analysis techniques

- different ciphertext symbols can represent the same plaintext symbol
  - *1 → many* relationship between letter and substitute

Leon Battista Alberti: 1466: *invented key*

- two disks
- line up predetermined letter on inner disk with outer disk
- plaintext on inner → ciphertext on outer
- after *n* symbols, the disk is rotated to a new alignment

encrypt: A→J

decrypt: J →A

Vigenère polyalphabetic cipher

- Blaise de Vigenère, court of Henry III of France, 1518
- Use table and key word to encipher a message
- repeat keyword over text: (e.g. key=FACE)

`FA CEF ACE FACEF ....`
`MY CAT HAS FLEAS`

- encrypt: find intersection:
  row = keyword letter
  column = plaintext letter
- decrypt: column = keyword letter, search for intersection = ciphertext letter
- message is encrypted with as many substitution ciphers as there are letters in the keyword

Vigenère polyalphabetic cipher

plaintext letter

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

keytext letter

ciphertext letter

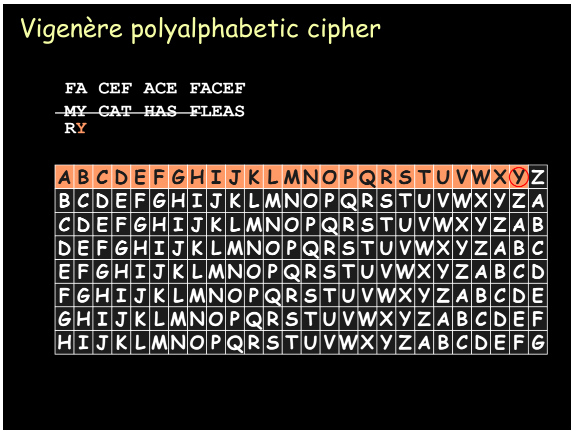
Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~**MY CAT HAS FLEAS**~~

R

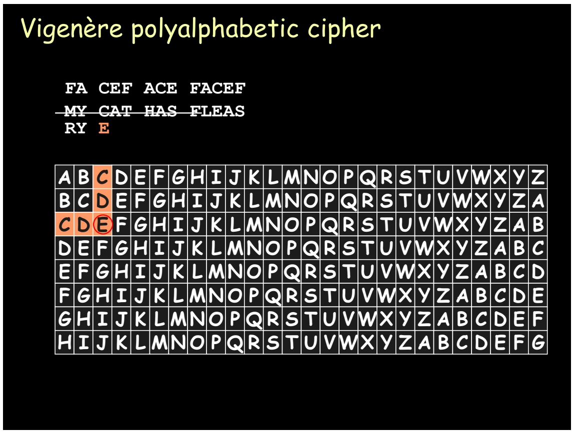
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY

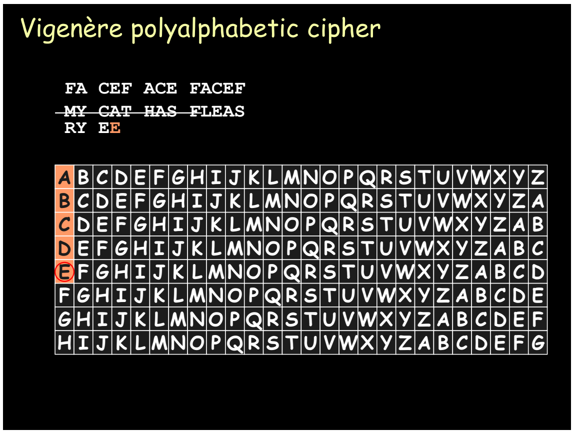
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY E

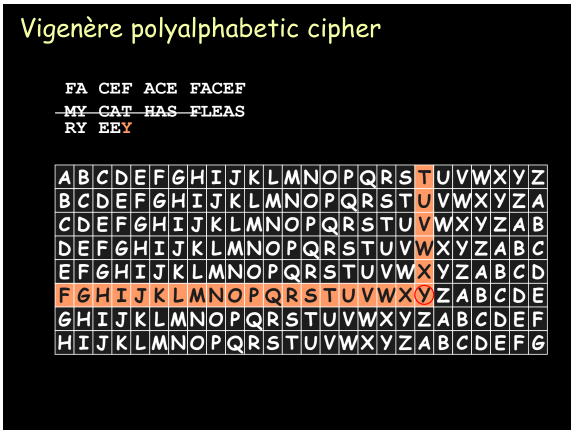
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EE

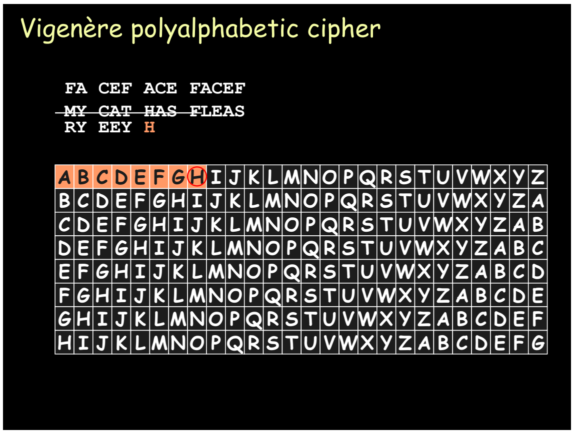
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY

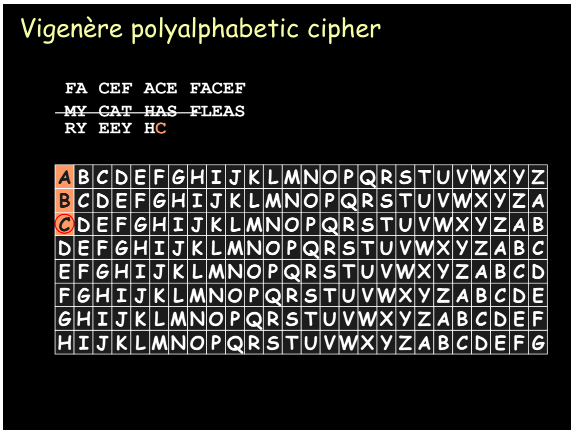
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY H

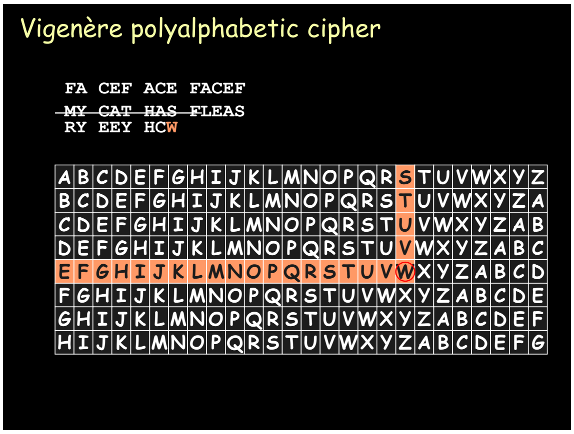
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY HC

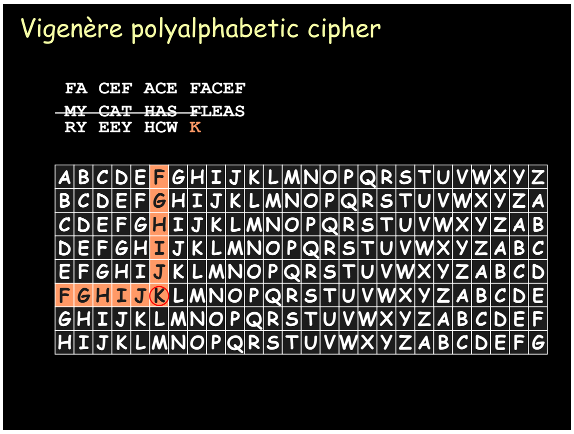
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY HCW

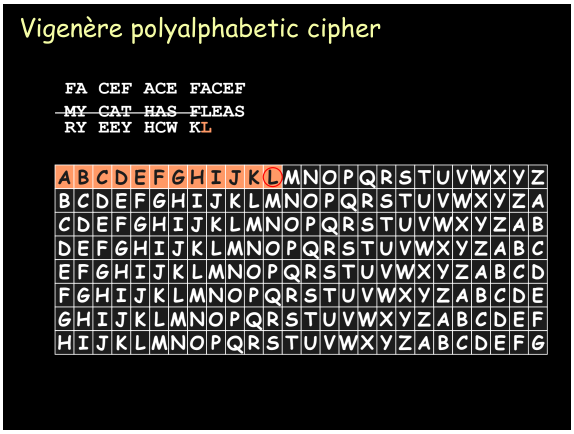
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY HCW K

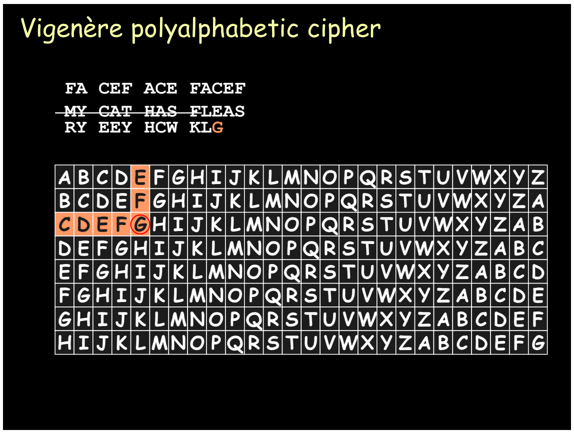
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY HCW KL

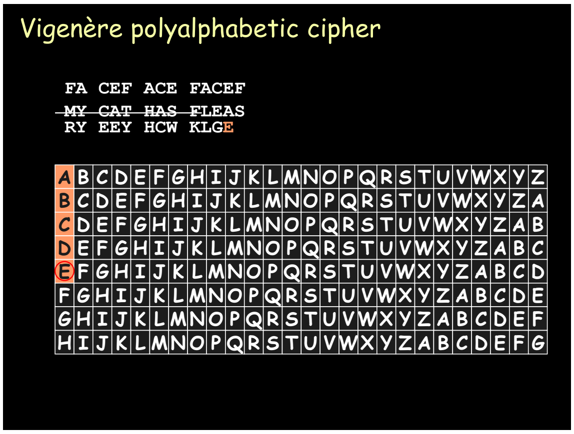
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY HCW KLG

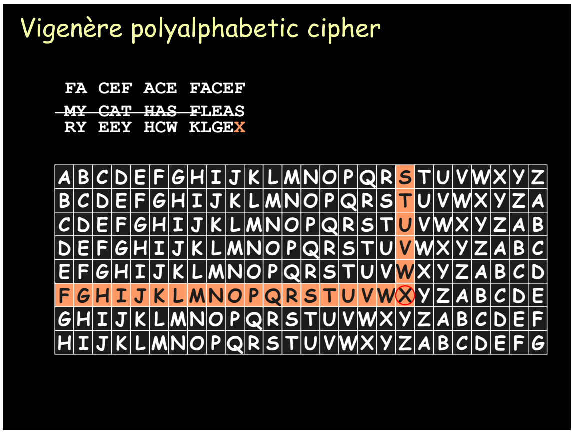
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY HCW KLGE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
~~MY CAT HAS FLEAS~~
RY EEY HCW KLGEX

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Vigenère polyalphabetic cipher

"The rebels reposed their major trust, however, in the Vigenere, sometimes using it in the form of a brass cipher disc. In theory, it was an excellent choice, for so far as the South knew the cipher was unbreakable. In practice, it proved a dismal failure. For one thing, transmission errors that added or subtracted a letter ... unmeshed the key from the cipher and caused no end of difficulty. Once Major Cunningham of General Kirby-Smith's staff tried for twelve hours to decipher a garbled message; he finally gave up in disgust and galloped around the Union flank to the sender to find out what it said."

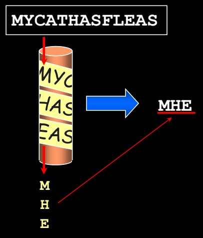
http://rz1.razorpoint.com/index.html

Transposition Ciphers

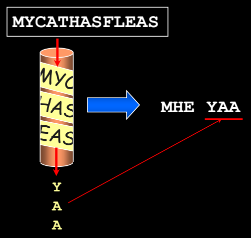
Transposition ciphers

- Permute letters in plaintext according to rules
- Knowledge of rules will allow message to be decrypted
- Earliest version used by the Spartans in the 5th century BC – staff cipher

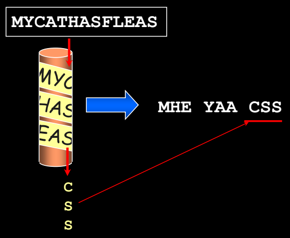
Transposition ciphers: staff cipher

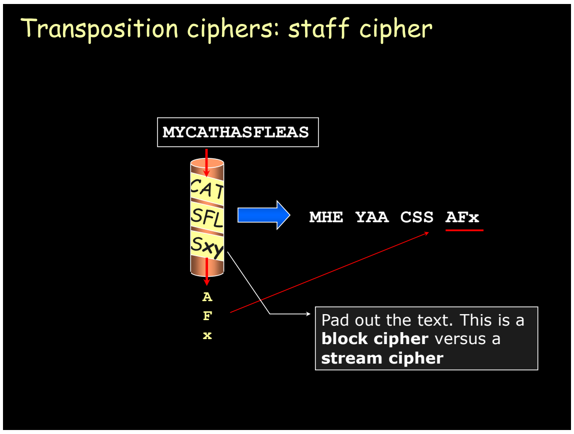


Transposition ciphers: staff cipher



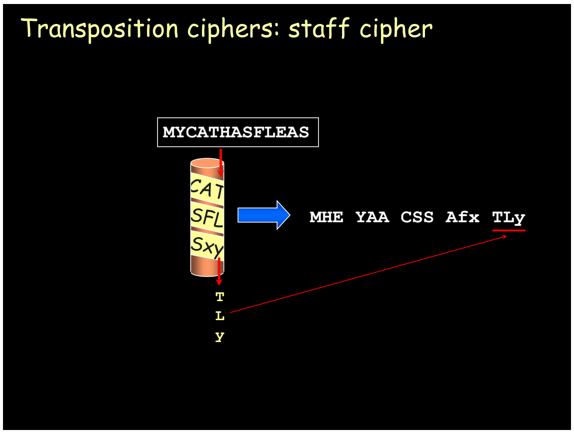
Transposition ciphers: staff cipher



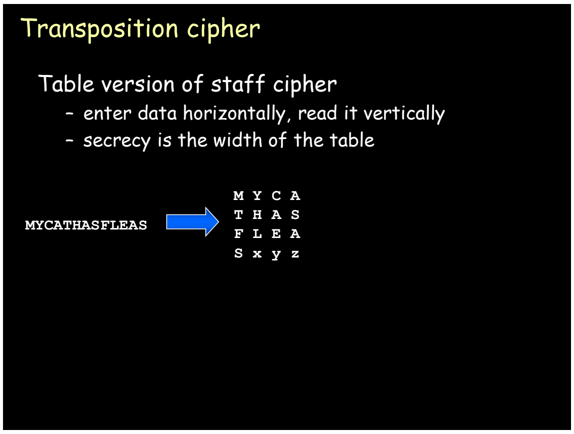


Transposition ciphers: staff cipher

Pad out the text. This is a **block cipher** versus a **stream cipher**

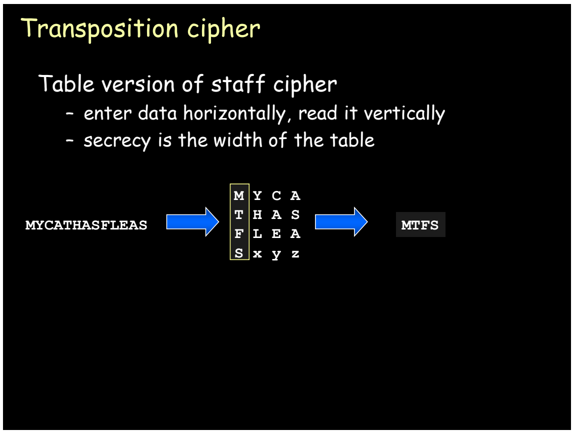


Transposition ciphers: staff cipher



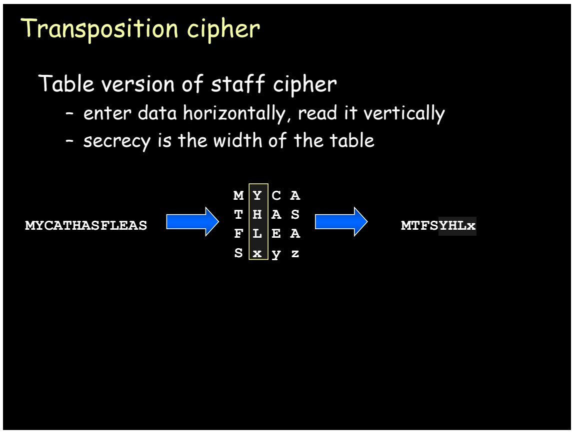
Transposition cipher

Table version of staff cipher
- enter data horizontally, read it vertically
- secrecy is the width of the table



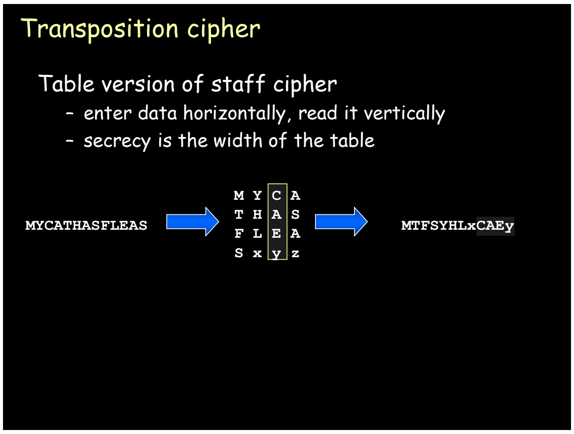
Transposition cipher

Table version of staff cipher
- enter data horizontally, read it vertically
- secrecy is the width of the table



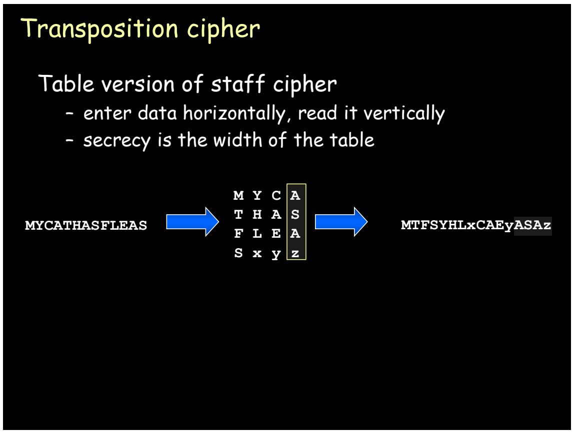
Transposition cipher

Table version of staff cipher
- enter data horizontally, read it vertically
- secrecy is the width of the table



Transposition cipher

Table version of staff cipher
- enter data horizontally, read it vertically
- secrecy is the width of the table



Transposition cipher

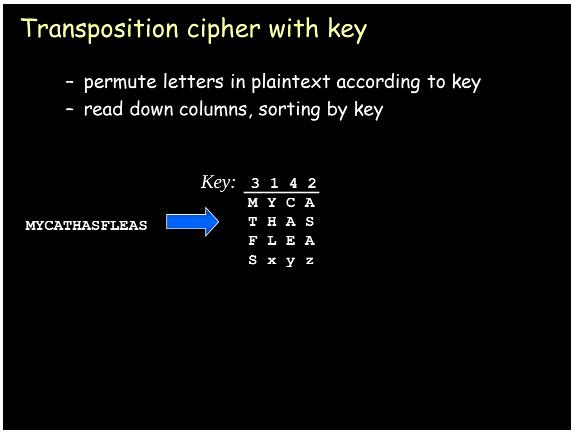
Table version of staff cipher

- enter data horizontally, read it vertically
- secrecy is the width of the table

MYCATHASFLEAS →

M Y C A
T H A S
F L E A
S x y z

→ MTFSYHLxCAEyASAz

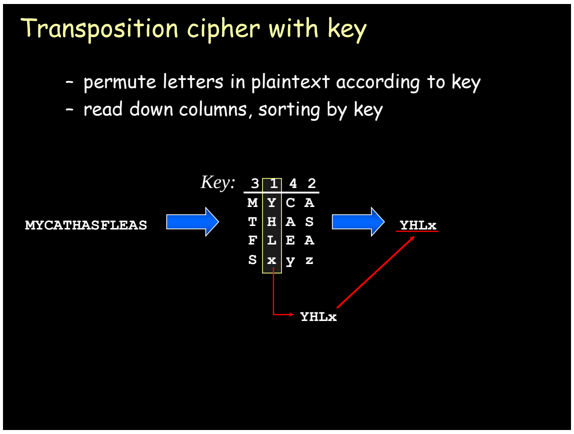


Transposition cipher with key

- permute letters in plaintext according to key
- read down columns, sorting by key

MYCATHASFLEAS →

Key: 3 1 4 2
M Y C A
T H A S
F L E A
S x y z



Transposition cipher with key

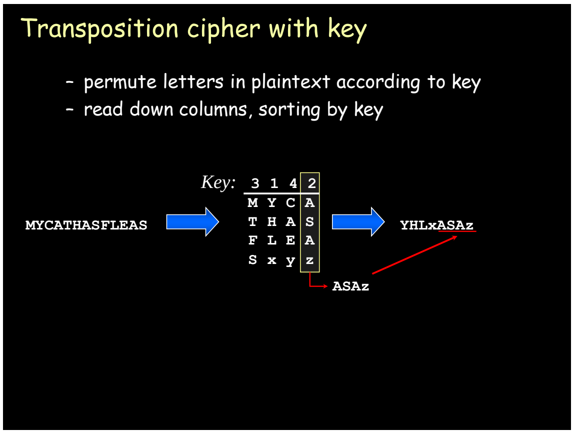
- permute letters in plaintext according to key
- read down columns, sorting by key

MYCATHASFLEAS →

Key: 3 1 4 2
M Y C A
T H A S
F L E A
S x y z

→ YHLx

YHLx



Transposition cipher with key

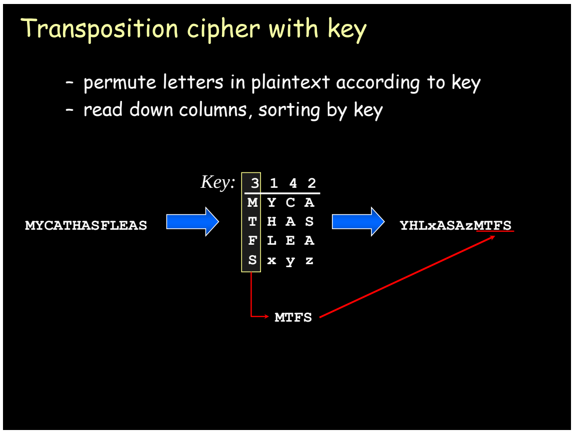
- permute letters in plaintext according to key
- read down columns, sorting by key

MYCATHASFLEAS →

Key: 3 1 4 2
M Y C A
T H A S
F L E A
S x y z

→ YHLxASAz

ASAz



Transposition cipher with key

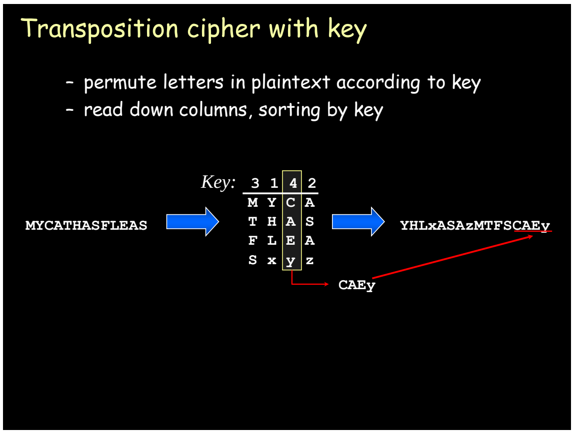
- permute letters in plaintext according to key
- read down columns, sorting by key

MYCATHASFLEAS →

Key: 3 1 4 2
M Y C A
T H A S
F L E A
S x y z

→ YHLxASAzMTFS

MTFS



Transposition cipher with key

- permute letters in plaintext according to key
- read down columns, sorting by key

MYCATHASFLEAS →

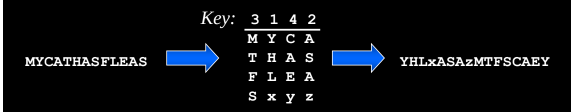
Key: 3 1 4 2
M Y C A
T H A S
F L E A
S x y z

→ YHLxASAzMTFSCAEy

CAEy

Transposition cipher with key

- permute letters in plaintext according to key
- read down columns, sorting by key



MYCATHASFLEAS

Key:

3	1	4	2
M	Y	C	A
T	H	A	S
F	L	E	A
S	x	y	z

YHLxASAzMTFSCAEY

Combined ciphers

- Combine transposition with substitution ciphers
  - German ADFGVX cipher (WWI)
- can be troublesome to implement
  - may require a lot of memory
  - may require that messages be certain lengths
- Difficult with manual cryptography

Electro-mechanical cryptographic engines

Rotor machines

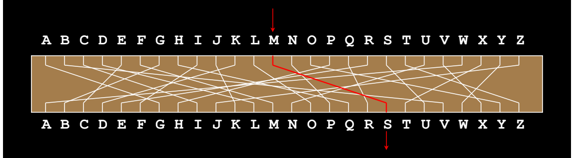
1920s: mechanical devices used for automating encryption

Rotor machine:

- set of independently rotating cylinders through which electrical pulses flow
- each cylinder has input & output pin for each letter of the alphabet
- implements a version of the Vigenère cipher
- each rotor implements a substitution cipher
- output of each rotor is fed into the next rotor

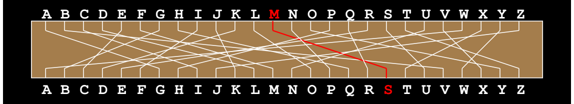
Rotor machines

- Simplest rotor machine: single cylinder

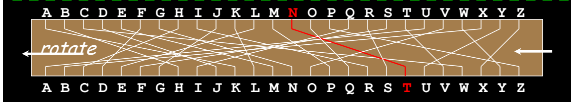


- after a character is entered, the cylinder rotates one position
  - internal combinations shifted by one
  - polyalphabetic substitution cipher with a period of 26

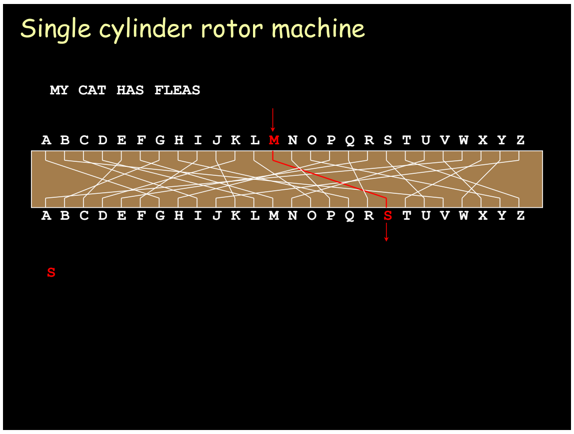
Single cylinder rotor machine



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	V	I	L	C	M	B	Q	F	K	D	O	S	P	Z	H	R	E	U	Z	N	X	A	T	W	J



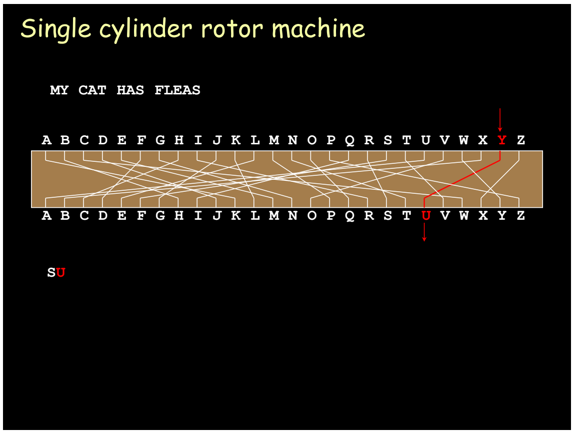
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	H	W	J	M	D	N	C	R	G	L	E	P	T	Q	Z	I	S	F	V	A	O	Y	B	U	X



Single cylinder rotor machine

MY CAT HAS FLEAS

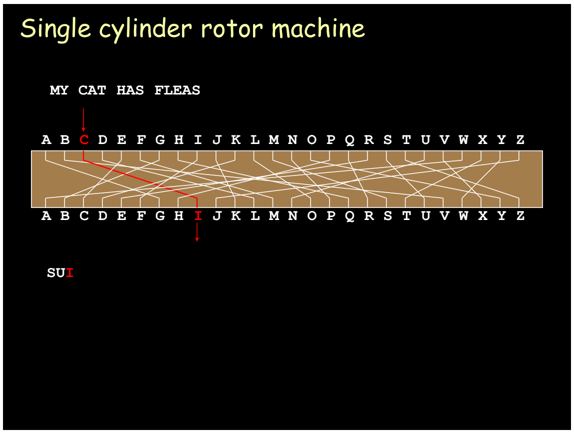
S



Single cylinder rotor machine

MY CAT HAS FLEAS

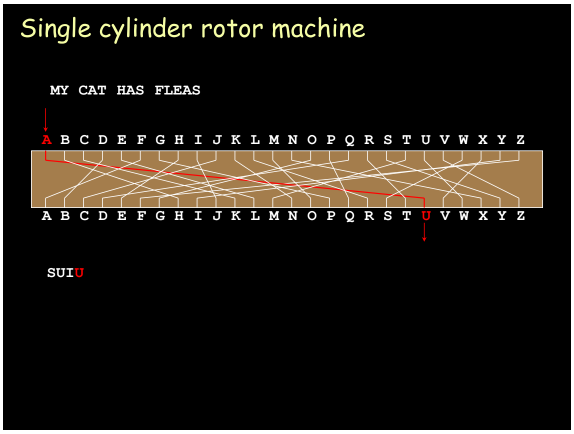
SU



Single cylinder rotor machine

MY CAT HAS FLEAS

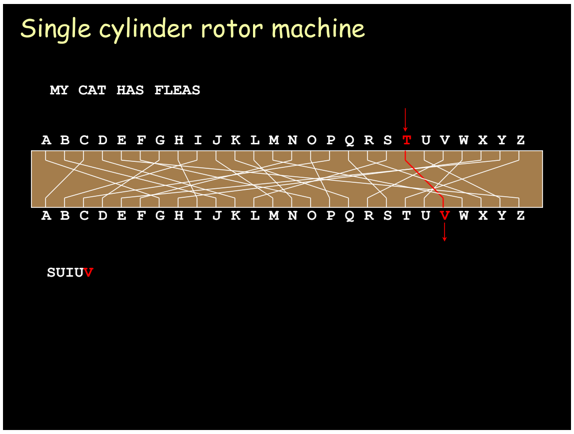
SUI



Single cylinder rotor machine

MY CAT HAS FLEAS

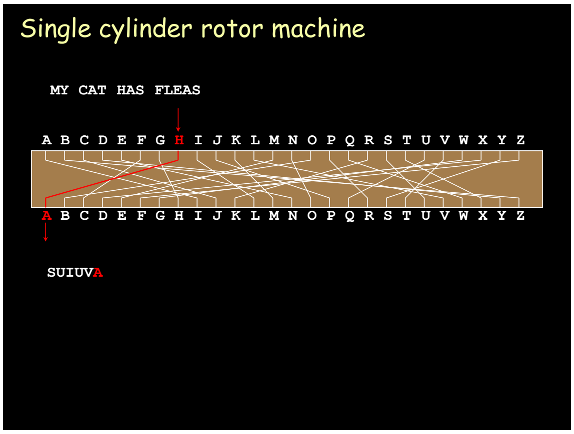
SUIU



Single cylinder rotor machine

MY CAT HAS FLEAS

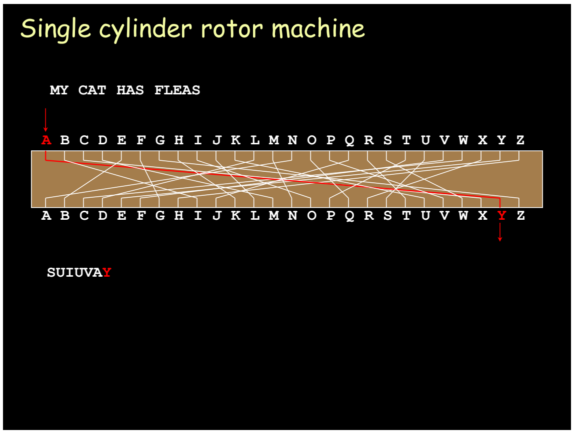
SUIUV



Single cylinder rotor machine

MY CAT HAS FLEAS

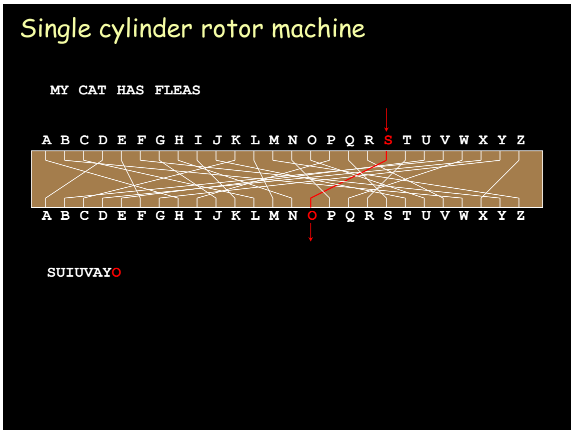
SUIUVA



Single cylinder rotor machine

MY CAT HAS FLEAS

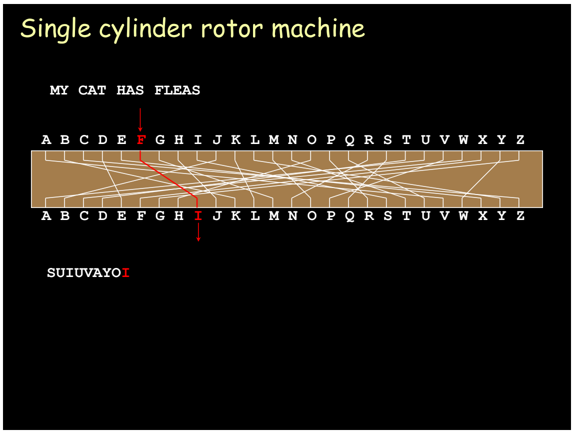
SUIUVAY



Single cylinder rotor machine

MY CAT HAS FLEAS

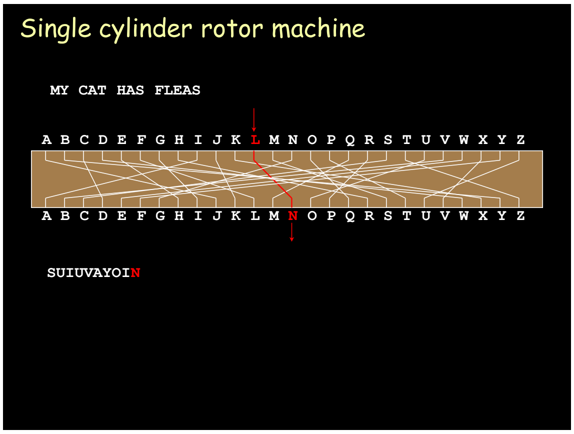
SUIUVAYO



Single cylinder rotor machine

MY CAT HAS FLEAS

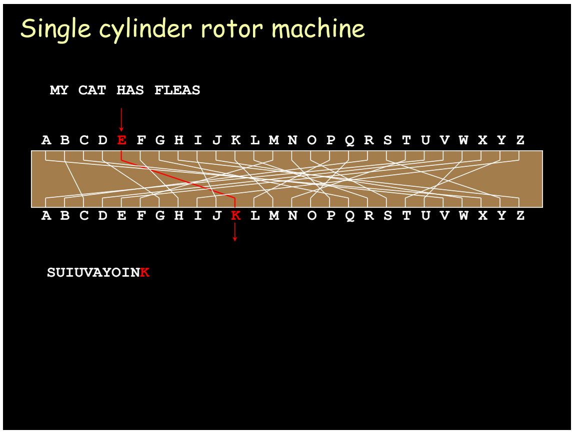
SUIUVAYOI



Single cylinder rotor machine

MY CAT HAS FLEAS

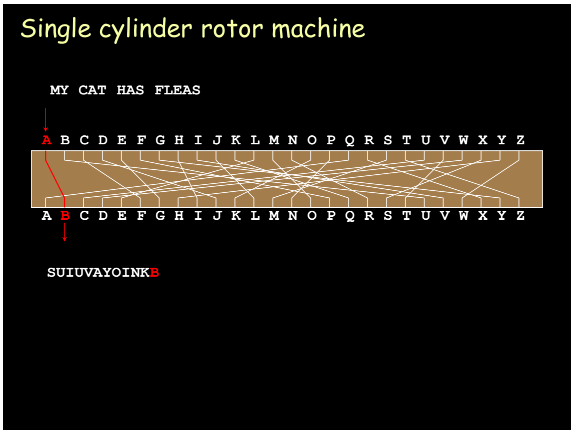
SUIUVAYOIN



Single cylinder rotor machine

MY CAT HAS FLEAS

SUIUVAYOINK



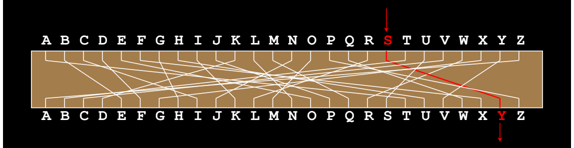
Single cylinder rotor machine

MY CAT HAS FLEAS

SUIUVAYOINKB

Single cylinder rotor machine

MY CAT HAS FLEAS



SUIUVAYOINKBY

Multi-cylinder rotor machines

Single cylinder rotor machine

- substitution cipher with a period = length of alphabet (e.g., 26)

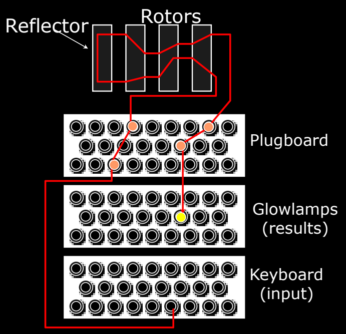
Multi-cylinder rotor machine

- feed output of one cylinder as input to the next one
- first rotor advances after character is entered
- second rotor advances after a full period of the first
- polyalphabetic substitution cipher
  - period = (length of alphabet)$^{\text{number of rotors}}$
  - 3 26-char cylinders ⇒ 26^3 = 17,576 substitution alphabets
  - 5 26-char cylinders ⇒ 26^5 = 11,881,367 substitution alphabets

Enigma

- Enigma machine used in Germany during WWII
- Three rotor system
  - 26^3 = 17,576 possible rotor positions
- Input data permuted via patch panel before sending to rotor engine
- Data from last rotor reflected back through rotors ⇒ *makes encryption symmetric*
- Need to know initial settings of rotor
  - setting was *f(date)*
  - find in book of codes
- broken by group at Bletchley Park (Alan Turing)

Enigma



One-time pads

Only provably secure encryption scheme

- invented in 1917
- large non-repeating set of random key letters written on a pad
- each key letter on the pad encrypts exactly one plaintext character
  - encryption is addition of characters modulo 26
- sender destroys pages that have been used
- receiver maintains identical pad

One-time pads

If pad contains

KWXOPWMAELGHW…

and we want to encrypt

MY CAT HAS FLEAS

Ciphertext:

WUZOIDMSJWKHO

M + K mod 26 = W
Y + W mod 26 = U
C + X mod 26 = Z
A + O mod 26 = O
T + P mod 26 = I
H + W mod 26 = D
A + M mod 26 = M
S + A mod 26 = S
F + E mod 26 = J
L + L mod 26 = W
E + G mod 26 = K
A + H mod 26 = H
S + W mod 26 = O

One-time pads

The same ciphertext can decrypt to *anything* depending on the key!

Same ciphertext:

WUZOIDMSJWKHO

With a pad of:

KWXOPWMAELGHW…

Produces:

THE DOG IS HAPPY

W - D mod 26 = W
U - N mod 26 = U
Z - V mod 26 = Z
O - L mod 26 = O
I - U mod 26 = I
D - X mod 26 = D
M - E mod 26 = M
S - A mod 26 = S
J - C mod 26 = J
W - W mod 26 = W
K - V mod 26 = K
H - S mod 26 = H
O - Q mod 26 = O

One-time pads

Can be extended to binary data

- random key sequence as long as the message
- exclusive-or key sequence with message
- receiver has the same key sequence

One-Time Pad

```
void onetimepad(void)
{
      FILE *if = fopen(“intext”, “r”);
      FILE *kf = fopen(“keytext”, “r”);
      FILE *of = fopen(“outtext”, “w”);
      int c, k;

      while ((c = getc(if)) != EOF) {
            k = getc(kf);
            putc((c^k), of);
      }
      fclose(if); fclose(kf); fclose(of);
}
```

One-time pads

Problems with one-time pads:

- key needs to be as long as the message!
- key storage can be problematic
    - may need to store a lot of data
- keys have to be generated randomly
    - cannot use pseudo-random number generator
- cannot reuse key sequence
- sender and receiver *must* remain synchronized (e.g. cannot lose a message)

Digression: random numbers

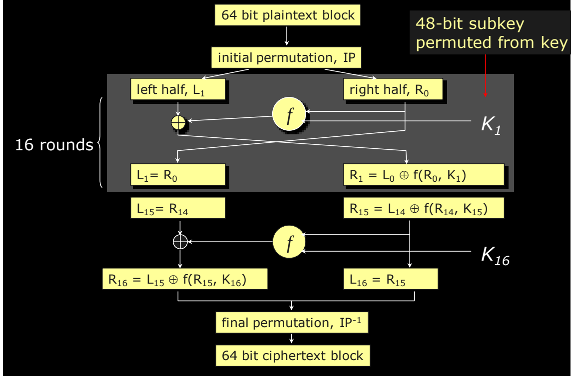
- “anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin”
    - John vonNeumann
- Pseudo-random generators
    - Linear feedback shift registers
    - Multiplicative lagged Fibonacci generators
    - Linear congruential generator
- Obtain randomness from:
    - Time between keystrokes
    - Various network/kernel events
    - Cosmic rays
    - Electrical noise
    - Other encrypted messages

Computer Cryptography

DES

- Data Encryption Standard
  - adopted as a federal standard in 1976
- block cipher, 64 bit blocks
- 56 bit key
  - all security rests with the key
- substitution followed by a permutation (transposition)
  - same combination of techniques is applied on the plaintext block 16 times

DES



64 bit plaintext block

initial permutation, IP

48-bit subkey permuted from key

16 rounds

left half, L_1

right half, R_0

$L_1= R_0$

$R_1 = L_0 \oplus f(R_0, K_1)$

$L_{15}= R_{14}$

$R_{15} = L_{14} \oplus f(R_{14}, K_{15})$

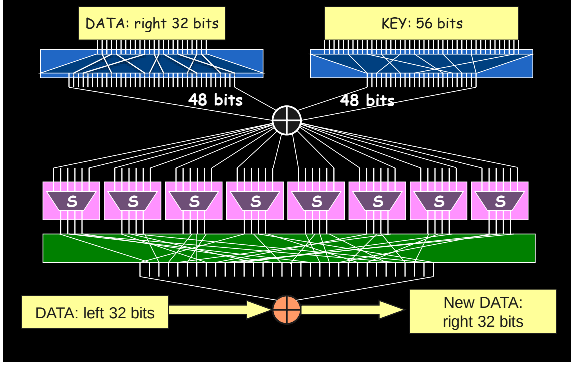
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$

$L_{16} = R_{15}$

final permutation, IP^{-1}

64 bit ciphertext block

DES: *f*



DATA: right 32 bits

KEY: 56 bits

DATA: left 32 bits

New DATA: right 32 bits

DES: S-boxes

- After compressed key is XORed with expanded block
  - 48-bit result moves to substitution operation via eight substitution boxes (s-boxes)
- Each S-box has
  - 6-bit input
  - 4-bit output
- 48 bits divided into eight 6-bit sub-blocks
- Each block is operated by a separate S-box
- key components of DES's security
- net result: 48 bit input generates 32 bit output

Is DES secure?

56-bit key makes DES relatively weak

- 7.2×10^{16} keys
- Brute-force attack

Late 1990's:

- DES cracker machines built to crack DES keys in a few hours
- DES Deep Crack: 90 billion keys/second
- Distributed.net: test 250 billion keys/second

The power of 2

Adding an extra bit to a key doubles the search space.

Suppose it takes 1 second to attack a 20-bit key:

- 21-bit key: 2 seconds
- 32-bit key: 1 hour
- 40-bit key: 12 days
- 56-bit key: 2,178 years
- 64-bit key: >557,000 years!

Increasing The Key

Can double encryption work for DES?

- Useless if we could find a key K such that:

  $E_K(P) = E_{K2}(E_{K1}(P))$

- This does not hold for DES

Double DES

Vulnerable to meet-in-the-middle attack

If we know some pair (P, C), then:

[1] Encrypt P for all 2^{56} values of K_1
[2] Decrypt C for all 2^{56} values of K_2

For each match where [1] = [2]

- test the two keys against another P, C pair
- if match, you are assured that you have the key

Triple DES

Triple DES with two 56-bit keys:

$C = E_{K1}(D_{K2}(E_{K1}(P)))$

Triple DES with three 56-bit keys:

$C = E_{K3}(D_{K2}(E_{K1}(P)))$

Decryption used in middle step for compatibility with DES (K_1=K_2=K_3)

$C = E_K(D_K(E_K(P))) \equiv C = E_{K1}(P)$

Triple DES

Prevent meet-in-the-middle attack with

- three stages
- and two keys

Triple DES:

$C = E_{K1}(D_{K2}(E_{K1}(P)))$

Decryption used in middle step for compatibility with DES

$C = E_K(D_K(E_K(P))) \equiv C = E_{K1}(P)$

Popular symmetric algorithms

IDEA - International Data Encryption Algorithm

- 1992
- 128-bit keys, operates on 8-byte blocks (like DES)
- algorithm is more secure than DES

RC4, by Ron Rivest

- 1995
- key size up to 2048 bits
- not secure against multiple messages encrypted with the same key

AES - Advanced Encryption Standard

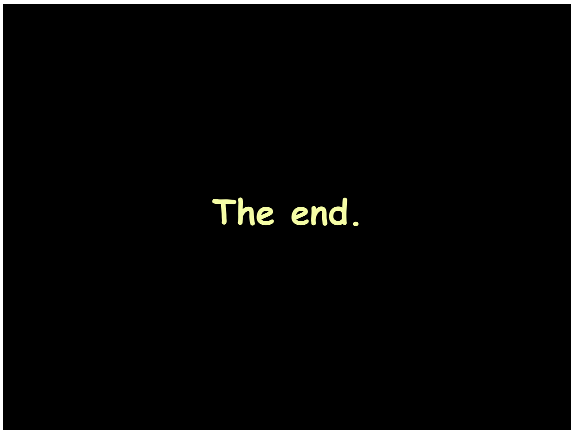
- NIST proposed successor to DES, chosen in October 2000
- based on Rigndael cipher
- 128, 192, and 256 bit keys

AES

From NIST:

Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{56} keys per second), then it would take that machine approximately 149 trillion years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old.

http://csrc.nist.gov/encryption/aes/



The end.